

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-208410

(43)Date of publication of application : 25.07.2003

(51)Int.Cl.

G06F 15/00
G06K 17/00

(21)Application number : 2002-008180

(71)Applicant : DAINIPPON PRINTING CO LTD

(22)Date of filing : 17.01.2002

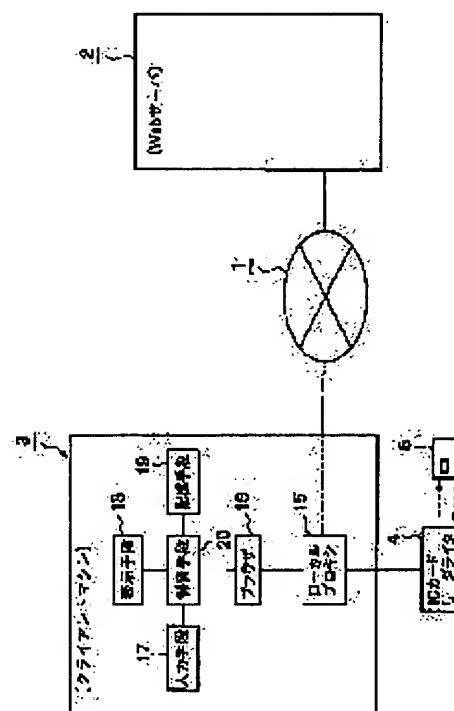
(72)Inventor : SAITO KENICHIRO

(54) AUTHENTICATION INFORMATION CREATING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an authentication information creating system capable of preventing the illegal access by a third person by allowing only a person having the access right to display a log-in form in which the log-in data is automatically inputted in advance.

SOLUTION: The authentication information creating system comprises an IC card storing the log-in data, an IC card reader/writer connected to a client machine, and the client machine having a local proxy for reading the log-in data stored in the IC card by the IC card reader/writer when the transmission of the log-in data is requested from a WEB server, and creating the display information of the log-in form in which the log-in data is inputted in advance by using the log-in data, and a browser receiving the display information of the log-in form from the local proxy for making a display means to display the display information of the log-in form.



LEGAL STATUS

[Date of request for examination]

14.01.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-208410

(P2003-208410A)

(43) 公開日 平成15年7月25日 (2003.7.25)

(51) Int.Cl. ⁷	識別記号	F I	特許出願公開番号
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 G 5 B 0 5 8
G 0 6 K 17/00		G 0 6 K 17/00	D 5 B 0 8 5

審査請求 未請求 請求項の数 2 O L (全 7 頁)

(21) 出願番号 特願2002-8180(P2002-8180)

(22) 出願日 平成14年1月17日 (2002.1.17)

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72) 発明者 斎藤 賢一郎

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

(74) 代理人 100111659

弁理士 金山 聡

Fターム(参考) 5B058 CA01 KA02 KA04 YA20

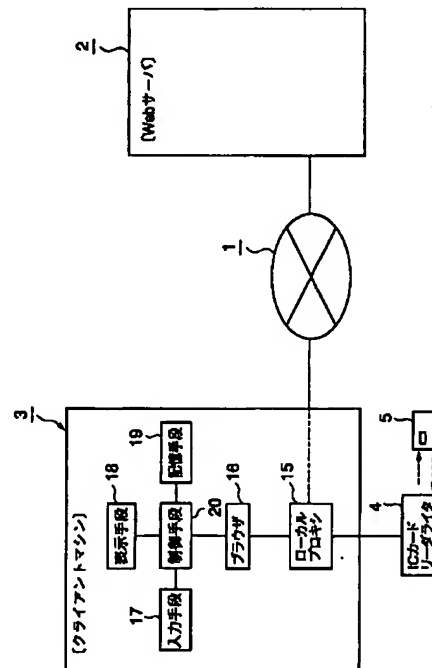
5B085 AE02 AE03 AE12 BE01

(54) 【発明の名称】 認証情報生成システム

(57) 【要約】

【課題】 アクセス権を有する本人だけが自動的に予めログインデータが入力されたログインフォームの表示を可能とさせるようにすることで、第三者による不正なアクセスを防止できるようにした認証情報生成システムを提供する。

【解決手段】 ログインデータが格納されているICカードと、クライアントマシンに接続されたICカードリーダーライタと、WEBサーバからログインデータの送信要求があった場合に、前記ICカードリーダーライタで前記ICカードに格納されているログインデータを読み取らせ、該ログインデータを用いて予め前記ログインデータが入力されたログインフォームの表示情報を生成するローカルプロキシと、前記ローカルプロキシから前記ログインフォームの表示情報を受信し、表示手段に前記ログインフォームの表示情報を表示させるブラウザとを有する前記クライアントマシンと、からなることを特徴とする。



【特許請求の範囲】

【請求項1】 HTTPアクセスを送信するクライアントマシンと、ネットワークを介して前記HTTPアクセスを受信した後、アクセス権を確認するためのログインデータの要求信号を前記クライアントマシンに送信するWEBサーバとにより、前記クライアントマシンが前記WEBサーバからログインデータの要求信号を受信した際における認証情報生成システムであって、前記アクセス権を確認するためのログインデータが格納されているICカードと、

前記クライアントマシンに接続され、前記ICカードに格納されているログインデータを読み取るICカードリーダーライターと、

前記WEBサーバからログインデータの送信要求があった場合に、前記ICカードリーダーライターで前記ICカードに格納されているログインデータを読み取らせ、該ログインデータを用いて予め前記ログインデータが入力されたログインフォームの表示情報を生成するローカルプロキシと、前記ローカルプロキシから前記ログインフォームの表示情報を受信し、表示手段に前記ログインフォームの表示情報を表示させるブラウザとを有する前記クライアントマシンと、

からなることを特徴とする認証情報生成システム。

【請求項2】 HTTPアクセスを送信するクライアントマシンと、ネットワークを介して前記HTTPアクセスを受信した後、アクセス権を確認するためのログインデータの要求信号を前記クライアントマシンに送信するWEBサーバとにより、前記クライアントマシンが前記WEBサーバからログインデータの要求信号を受信した際における認証情報生成システムであって、複数種類のURLと、前記各URL毎に対応したアクセス権を確認するためのログインデータが格納されているICカードと、

前記クライアントマシンに接続され、前記ICカードに格納されているURLとログインデータを読み取るICカードリーダーライターと、

前記WEBサーバからログインデータの送信要求があった場合に、前記ICカードリーダーライターで前記ICカードに格納されている複数種類のURLの中から、その送信要求があったURLに対応して記憶されているログインデータを読み取らせ、該ログインデータを用いて予め前記ログインデータが入力されたログインフォームの表示情報を生成するローカルプロキシと、前記ローカルプロキシから前記ログインフォームの表示情報を受信し、表示手段に前記ログインフォームの表示情報を表示させるブラウザとを有する前記クライアントマシンと、からなることを特徴とする認証情報生成システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、通信ネットワーク

上の情報にアクセスし、このアクセス権を確認するためのログインデータの要求信号がWEBサーバからクライアントマシンに送信された際に、前記クライアントマシンで前記WEBサーバに送信するためのログインデータを自動的に生成する認証情報生成システムに関する。

【0002】 従来、パソコン等のクライアントマシンを利用してインターネットに接続し、会員制などのサービスを受ける場合には、通常、Webブラウザを起動させ、キーボード等の入力手段から見たいホームページのURLを入力したり、またはブックマークに記録してあればそのURLを指定してURLを入力して、WEBサーバにアクセスを行なう。その後、WEBサーバからクライアントマシンに対して、ユーザIDやパスワード等の認証情報からなるログインデータの送信を要求する情報が送信され、これらのログインデータをクライアントマシンからWEBサーバに送信し、照合判定を経た後に所定のサービスを受けることが可能となるようにしてある。

【0003】 一般的に、クライアントマシンのWEBブラウザの機能として、前回のログイン時のログインデータを記憶しておき、次回以降におけるWEBサーバからクライアントマシンに対するログインデータの送信要求があった際に、これらの記憶されているデータを自動的に用いることで、WEBサーバからログインデータの送信要求があった場合にその都度キーボード等の入力手段からユーザIDやパスワード等を入力しなくても処理できるようにして入力作業の手間を省くことを可能にしていることが多い。

【0004】 しかしながら、WEBブラウザの機能によっては、自動的にログインデータが入力される場合に、認証情報がソフトウェアで処理されるため、ログインデータが盗難される恐れがある。また、ユーザがブラウザを適切に設定していない場合、他人がブラウザを操作した時に、前回ユーザがログインした時のデータが自動的に入力されるため、第三者によるログインが容易となり、不正なアクセスが行われる危険性がある。

【0005】 更に、ブラウザ機能によるサポートがない場合、異なる複数のログインの要求に対してのアクセスを行なうには、それぞれの要求に対応したログインデータをキーボード等から入力しなければならず、手間がかかり、またこれらのログインデータをメモ書きなどの記録で管理しておくこともありセキュリティ上の問題がある。

【0006】

【発明が解決しようとする課題】 本発明は、クライアントマシンがWEBサーバからログインデータの要求信号を受信した際に、アクセス権を有する本人だけが自動的に予めログインデータが入力されたログインフォームの表示を可能とさせるようにすることで、第三者による不正なアクセスを防止できるようにした認証情報生成シ

テムを提供する。更に、本発明は、異なる複数の要ログインの要求に対してのアクセスを行なう場合でも、それぞれの要求に対応したログインデータをキーボード等から入力しなくても、自動的にそれらに対応したログインデータが予め入力されたログインフォームの表示を可能とした認証情報生成システムを提供する。

【0007】

【課題を解決するための手段】本発明の認証情報生成システムは、HTTPアクセスを送信するクライアントマシンと、ネットワークを介して前記HTTPアクセスを受信した後、アクセス権を確認するためのログインデータの要求信号を前記クライアントマシンに送信するWEBサーバとにより、前記クライアントマシンが前記WEBサーバからログインデータの要求信号を受信した際における認証情報生成システムであって、前記アクセス権を確認するためのログインデータが格納されているICカードと、前記クライアントマシンに接続され、前記ICカードに格納されているログインデータを読み取るICカードリーダーライタと、前記WEBサーバからログインデータの送信要求があった場合に、前記ICカードリーダーライタで前記ICカードに格納されているログインデータを読み取らせ、該ログインデータを用いて予め前記ログインデータが入力されたログインフォームの表示情報を生成するローカルプロキシと、前記ローカルプロキシから前記ログインフォームの表示情報を受信し、表示手段に前記ログインフォームの表示情報を表示させるブラウザとを有する前記クライアントマシンと、からなることを特徴とする。

【0008】また、本発明の認証情報生成システムは、HTTPアクセスを送信するクライアントマシンと、ネットワークを介して前記HTTPアクセスを受信した後、アクセス権を確認するためのログインデータの要求信号を前記クライアントマシンに送信するWEBサーバとにより、前記クライアントマシンが前記WEBサーバからログインデータの要求信号を受信した際における認証情報生成システムであって、複数種類のURLと、前記各URL毎に対応したアクセス権を確認するためのログインデータが格納されているICカードと、前記クライアントマシンに接続され、前記ICカードに格納されているURLとログインデータを読み取るICカードリーダーライタと、前記WEBサーバからログインデータの送信要求があった場合に、前記ICカードリーダーライタで前記ICカードに格納されている複数種類のURLの中から、その送信要求があったURLに対応して記憶されているログインデータを読み取らせ、該ログインデータを用いて予め前記ログインデータが入力されたログインフォームの表示情報を生成するローカルプロキシと、前記ローカルプロキシから前記ログインフォームの表示情報を受信し、表示手段に前記ログインフォームの表示情報を表示させるブラウザとを有する前記クライアント

マシンと、からなることを特徴とする。

【0009】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。図1は、本発明の一実施形態に係る認証情報生成システムの概略構成を示す図、図2は、本発明に使用するICカードのブロック図、図3は、本発明に使用するICカードの記憶内容を示す図、図4は、本発明の一実施形態に係る認証情報自動生成システムの概略的なブロック図、図5は、本発明の一実施形態に係る認証情報生成システムのクライアントマシンにおけるログイン画面の一例を示す図、図6は、本発明の一実施形態に係る認証情報生成システムの処理手順を示すフローチャートである。

【0010】図1に示すように、インターネット1上には、種々のサービスや情報を提供する複数のWebサーバ2a、2bが接続されると共に、これらのWebサーバ2a、2bからサービスや情報の提供を受けるためのパソコン等からなるクライアントマシン3が接続されている。このクライアントマシン3には、ICカードリーダーライタ4が接続され、ICカードリーダーライタ4にセットされたICカード5に記憶されたデータの読み取りを可能にしてある。

【0011】ICカード5には、図2に示すように、制御手段であるCPU6、記憶手段として備えられた読み出し専用メモリ(ROM)7aと、書き換え可能な不揮発性メモリ(EEPROM)7bと、揮発性メモリ(RAM)7cとを有する。また、更にICカード5には、電源電圧を供給するVCC端子8、接地用のGND端子9、リセット信号を供給するRST端子10、クロック信号を供給するCLK端子11、データ入出力手段であるI/O端子12とがそれぞれ備えられている。そして、上記のCPUと各メモリと各端子は、ICモジュール化されてカード基材に埋設された構成を有している。

【0012】また、不揮発性メモリ(EEPROM)7bには、図3に示すような内容の情報が記憶されている。この記憶情報としては、インターネットを介して接続されるWebサーバのホームページのアドレスであるURL13aと、このアドレスに接続する際に必要な認証情報として予めWebサーバ側に登録してあるユーザID13b及びパスワード13cとが関連情報として記憶されている。

【0013】更に、クライアントマシンの利用者が複数のWebサーバからサービスや情報の提供を受ける場合には、必要に応じてその他のWebサーバのホームページのアドレスであるURL14aと、このアドレスに接続する際に必要な認証情報として予めWebサーバ側に登録してあるユーザID14b及びパスワード14cなどを記憶させる。これにより利用者は、1枚のICカード5をICカードリーダーライタ4にセットするだけで、複数のWebサーバに対応したログインデータの自動入

力処理を行なうことができる。

【0014】次に、図5のブロック図に基づいて、本発明のシステム構成を説明する。クライアントマシン3には、ユーザ接続のインターネット・ゲートウェイ端部において、ローカルプロキシ(proxy)15というアプリケーションと、Webブラウザプログラム16とが備えられている。また、更にキーボード等からなる入力手段17と、CRT等の表示手段18と、記憶手段19と、制御手段20とを備えている。

【0015】クライアントマシン3とWebサーバ2との間の通信は、ローカルプロキシ15を経て行われ、ローカルプロキシ15からの要求に基づいてICカードリーダー4がICカード5に記憶された所望の情報を読み取り、この情報をローカルプロキシ15へ送信するようにしてある。つまり、利用者がWebサーバ2からサービスや情報の提供を受ける際において、クライアントマシン3の入力手段17からURLの入力または画面上からURLを特定する指示情報を入力し、ブラウザを起動することでこのURLとブラウザの情報とをローカルプロキシ15を経て、インターネット1を介してWebサーバ2に送信する。

【0016】また、これらの情報を受信したWebサーバ2では、要求されたURLに該当するホームページをクライアントマシン3に送信する前提として、利用者の認証情報の照合が必要な場合には、Webサーバ2からクライアントマシン3に対して、利用者のユーザIDやパスワード等の認証情報からなるログインデータの送信を要求するためのログイン要求情報が送信される。

【0017】ローカルプロキシ15では、Webサーバ2から受信したデータとして、ログインデータを入力する必要があるとするログイン要求情報が含まれている場合には、ICカードリーダー4に対して、ICカード5に記憶されたユーザID14b及びパスワード14cなどの認証情報を読み取らせて、ローカルプロキシ15に送信させる機能を有する。また、Webサーバ2から受信したデータにログイン要求情報が含まれていない場合には、そのデータはそのままをブラウザ16に送られる。

【0018】そして、ローカルプロキシ15は、サーバから受信したデータを編集したログインフォームに、ICカード5から読み出した認証情報を使用して、既にユーザIDやパスワード等の認証情報が設定された状態のログインフォームを作成し、ブラウザ16に送信する機能を有している。ブラウザ16は、ローカルプロキシ15から受信した既に認証情報が設定された状態のログインフォームを表示手段18により、図5に示すようなログイン画面21として表示させる。

【0019】図5に示すログイン画面21では、ユーザID表示部22やパスワード表示部23等の認証情報の

表示部と、これらの情報をログインデータとして、クライアントマシン3からWebサーバ2に送信することを認めるためのログイン送信ボタン24が表示される。尚、ログイン画面21のパスワード表示部23には、セキュリティ上の安全性を考慮して具体的な文字や番号の表示が行われないようにしておく。

【0020】また、クライアントマシン3が複数種類の異なるURLとアクセスする場合においては、各URL毎に対応したアクセス権を確認するための認証情報であるログインデータをICカード5に格納しておく。つまり、図3において、記憶情報としてインターネットを介して接続されるWebサーバのホームページのアドレスであるURL13aと、このアドレスに接続する際に必要な認証情報として予めWebサーバ側に登録してあるユーザID13b及びパスワード13cとが関連情報として記憶され、また別のWebサーバのホームページのアドレスであるURL14aと、このアドレスに接続する際に必要な認証情報であるユーザID14b及びパスワード14cとが関連情報として記憶させておく。

【0021】この場合、ローカルプロキシ15では、Webサーバ2から受信したデータ又はWebサーバ2から送信した際のデータの中から、WebサーバのホームページのアドレスであるURLを特定しておき、もしWebサーバ2から受信したデータにログイン要求情報が含まれている場合には、ICカードリーダー4に対して、ICカード5に記憶されたURLに対応して記憶されたユーザID及びパスワードなどの認証情報を読み取らせて、ローカルプロキシ15に送信させる機能を有する。これにより、1枚のICカードにより複数の異なるURLに対応することが可能となる。

【0022】次に、図6のフローチャートを参照して、本発明の一実施形態における認証情報生成システムの処理手順を説明する。まず、利用者は、自分のICカード5をICカードリーダー4にセットする(S1)。そして、クライアントマシン3の入力手段17から、アクセスを行いたいホームページのURLの入力又はブックマークに登録してあるURLの指定入力を行ない、このURLをWebサーバ2に送信する(S2)。これの対し、Webサーバ2からクライアントマシン3に対して、利用者のユーザIDやパスワード等の認証情報からなるログインデータの送信を要求するためのログイン要求情報が送信される(S3)。

【0023】そのログイン要求情報を受信したクライアントマシン3のローカルプロキシ15は、ICカードリーダー4に対して、ICカード5に記憶されたこのURLに関連させて記憶されたユーザID及びパスワードなどの認証情報を読み取らせて、送信させる(S4)。この認証情報を受信したクライアントマシン3のローカルプロキシ15は、サーバから受信したデータを編集したログインフォームに、ICカード5から読み出

した認証情報を使用して、既にユーザIDやパスワード等の認証情報が設定された状態のログインフォームを作成し、ブラウザ16に送信する(S5)。

【0024】ブラウザ16では、表示手段18に認証情報が設定された状態のログインフォームが表示されたログイン画面を映す(S6)。利用者は、このログイン画面のログインフォームを確認し、OKであれば「ログイン」の表示部分をクリックする(S7)。クライアントマシン3からWebサーバ2に対して、これらのユーザIDやパスワード等の認証情報からなるログインデータ10が送信される(S8)。以上の手順により、ログイン処理の際に利用者のICカード5に記憶されたユーザID及びパスワードなどの認証情報を読み取らせて、ログインデータとして用いることができるものである。

【0025】

【発明の効果】以上説明したように、本発明の認証情報生成システムは、クライアントマシンがWEBサーバからログインデータの要求信号を受信した際に、利用者が所持するICカードに記憶された認証情報を利用して、自動的に予めログインデータが入力されたログインフォームが表示されたログイン画面を表示手段に映し出すことができ、このログイン画面からログインデータの送信指示を行なうことができるので、第三者による不正なアクセスを防止することができるという効果がある。更に、本発明は、ICカードに異なる複数のURLに対応させた認証情報を記憶させているので、複数の異なる要ログインの要求に対しても、それぞれの要求に対応したログインデータをキーボード等から入力しなくても、自動的にログインデータが予め入力されたログインフォームをログイン画面に表示することができるので、第三者30による不正なアクセスを防止すると共に、作業効率がよいという効果がある。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る認証情報生成システムの概略構成を示す図である。

【図2】本発明に使用するICカードのブロック図である。

【図3】本発明に使用するICカードの記憶内容を示す図である。

【図4】本発明の一実施形態に係る認証情報生成システムの概略的なブロック図である。

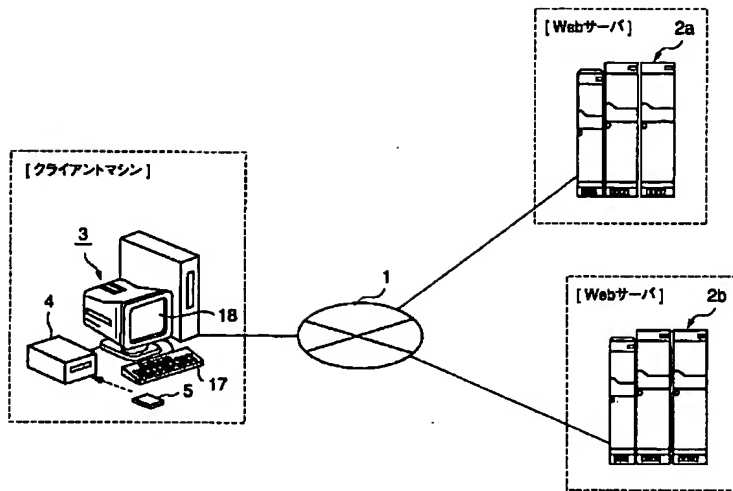
【図5】本発明の一実施形態に係る認証情報生成システムのクライアントマシンにおけるログイン画面の一例を示す図である。

【図6】本発明の一実施形態に係る認証情報生成システムの処理手順を示すフローチャートである。

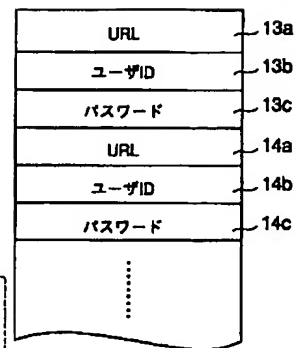
【符号の説明】

- 1 インターネット
- 2 a, 2 b Webサーバ
- 3 クライアントマシン
- 4 ICカードリーダライタ
- 5 ICカード
- 6 CPU
- 7 a 読み出し専用メモリ(ROM)
- 7 b 不揮発性メモリ(EEPROM)
- 7 c 揮発性メモリ(RAM)
- 8 VCC端子
- 9 GND端子
- 10 RST端子
- 11 CLK端子
- 12 I/O端子
- 13 a URL
- 13 b ユーザID
- 13 c パスワード
- 14 a URL
- 14 b ユーザID
- 14 c パスワード
- 15 ローカルプロキシ
- 16 ブラウザ
- 17 入力手段
- 18 表示手段
- 19 記憶手段
- 20 制御手段
- 21 ログイン画面
- 22 ユーザID表示部
- 23 パスワード表示部
- 24 ログイン送信ボタン

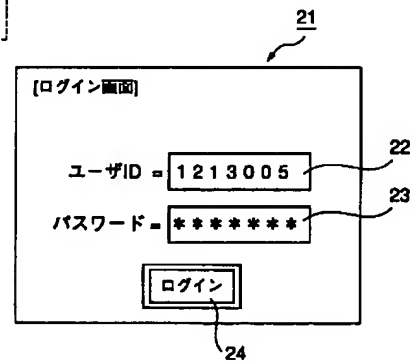
【図1】



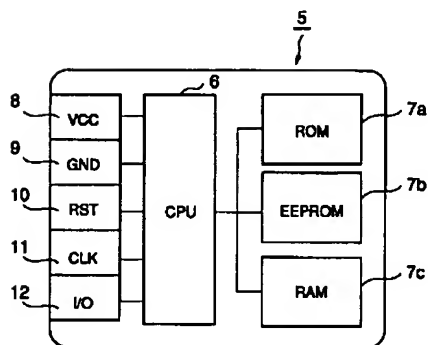
【図3】



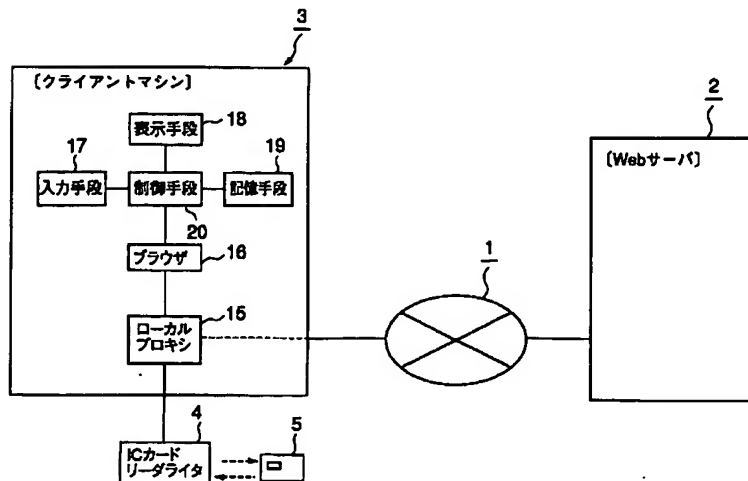
【図5】



【図2】



【図4】



【図6】

